COHN LIFLAND PEARLMAN HERRMANN & KNOPF LLP
Peter S. Pearlman
Park 80 West - Plaza One
250 Pehle Avenue, Suite 401
Saddle Brook, NJ 07663
Tel.: (201) 845-9600
Fax: (201) 845-9423
psp@njlawfirm.com

BERGER MONTAGUE, PC
Sherrie Savett
Shanon Carson
Jon Lambiras
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel.: (215) 875-3000
Fax: (215) 875-4604
ssavett@bm.net
scarson@bm.net
jlambiras@bm.net

Counsel for Plaintiff and the Classes

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

FRANCIS CARBONNEAU, on behalf of himself and all others similarly situated, Plaintiff, vs. QUEST DIAGNOSTICS INCORPORATED, AMERICAN MEDICAL COLLECTION AGENCY, INC., and OPTUM360, LLC, Defendants.	Case No.: _____ Civil Action **CLASS ACTION COMPLAINT & DEMAND FOR JURY TRIAL**

Plaintiff Francis Carbonneau ("Plaintiff") residing at Killdeer Island Road, Webster MA 01570, on behalf of himself and all others similarly situated, alleges the following against Defendants Quest Diagnostics Incorporated ("Quest"), American Medical Collection Agency, Inc. ("AMCA"), and Optum360, LLC ("Optum360") (collectively, "Defendants").

I. INTRODUCTION

1. This is a data breach class action on behalf of 11.9 million patients whose sensitive personal information was accessed by computer hackers in a cyber-attack (the "Data Breach"). Information compromised in the Data Breach includes Social Security numbers, financial information (*e.g.*, credit card numbers and bank account information), medical information, other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personal information (collectively, "Sensitive Information").

2. Plaintiff brings this class action lawsuit on behalf of a Nationwide Class and a Massachusetts Sub-Class (together, the "Classes") to address Defendants' inadequate safeguarding of class members' Sensitive Information.

3. Armed with the Sensitive Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

4. As a result of the Data Breach, Plaintiff and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

5. Plaintiff and class members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

6. Plaintiff seeks to remedy these harms on behalf of himself and all similarly-situated individuals whose Sensitive Information was accessed during the Data Breach.

7. Plaintiff seeks remedies including but not limited to compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and free credit monitoring services funded by Defendants.

II. PARTIES

8. Plaintiff Francis Carbonneau is an individual residing in Massachusetts. He has been a patient of Quest within the past year. His Sensitive Information, on information and belief, was compromised in the data breach.

9. Defendant Quest Diagnostics Inc. is incorporated in Delaware. Its principal place of business is in Secaucus, New Jersey.

10. Defendant American Medical Collection Agency, Inc. ("AMCA") is incorporated in Minnesota. Its principal place of business is in Elmsford, New York.

11. Defendant Optum360, LLC is incorporated in Delaware. Its principal place of business is in Eden Prairie, Minnesota.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the class are citizens of states different from Defendants.

13. This Court has personal jurisdiction over Defendants because Defendants conduct business in and throughout New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Venue is

also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Quest is headquartered in this District and all defendants are residents for venue purposes because they regularly transact business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because all Defendants are subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

15. Quest is the world's leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

16. On June 3, 2019, Quest publicly announced the following, in relevant part, in a Form 8-K filed with the Securities and Exchange Commission:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. . . . AMCA has informed Quest Diagnostics and Optum360 that:
>
> - between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
>
> - the information on AMCA's affected system included **financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers)**; [and]
>
> - as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately **11.9 million people** . . . .

17. Defendant AMCA failed to properly safeguard class members' Sensitive Information, allowing hackers to access their Sensitive Information for eight months. AMCA also

failed to properly monitor its systems. Had it properly monitored its systems, it would have discovered the intrusion much sooner than eight months after the breach began.

18. Defendant Quest failed to properly monitor its vendors – Defendant Optum360 and its sub-vendor Defendant AMCA – to ensure that proper data security safeguards were being implemented by those vendors throughout the breach period. Defendant Optum360 failed to properly monitor its vendor, Defendant AMCA, to ensure that proper data security safeguards were being implemented during the breach period.

19. Defendants had obligations created by HIPAA, industry standards, common law, and representations made to class members, to keep class members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

20. Plaintiff and class members provided their Sensitive Information to Quest with the reasonable expectation and mutual understanding that Quest and any business partners to which Quest disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized access.

21. Indeed, Quest promised patients that it will keep their Sensitive Information confidential, stating in its Notice of Privacy Practices that it is "committed to protecting the privacy of your identifiable health information."[1] Quest's Notice of Privacy Practices also acknowledged that Quest is subject to HIPAA.[2]

22. Quest further stated in its Notice of Privacy Practices that its vendors maintain adequate data security over patient data, stating:

> We may provide your PHI [Private Health Information] to other companies or individuals that need the information to provide

[1] *See* https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html.

[2] *Id.*

> services to us. These other entities, known as "business associates," are required to maintain the privacy and security of PHI.[3]

23. Defendants' data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach. The increase in data breaches, and attendant risk of future breaches, was widely known to the public and to anyone in Defendants' industries, including Defendants.

1. Defendants' Data Security Failures and HIPAA Violations

24. Defendants' data security failures demonstrate that they failed to honor their duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting patients' Sensitive Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that their vendors employed reasonable data security procedures;

e. Ensuring the confidentiality and integrity of electronic protected health information ("PHI") they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

[3] *Id.*

h. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

l. Training all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

2. Damages to Class Members

25. Plaintiff and class members have been damaged by the compromise of their Sensitive Information in the Data Breach.

26. Plaintiff and class members face a substantial risk of out of pocket fraud losses such as, *e.g.*, loans opened in their names, medical services billed in their name, tax return fraud, utility bills opened in their name, credit card fraud, and similar identity theft.

27. Class members may also incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

28. Plaintiff and class members suffered a "loss of value" of their Sensitive Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

29. Class members who paid Quest for its services were also damaged via "benefit of the bargain" damages. Such class members overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price class members paid to Quest was intended to be used by Quest to fund adequate data security and monitor its vendors' compliance with data security obligations. Quest did not properly monitor its vendors' compliance with data security obligations. Thus, the class members did not get what they paid for.

30. Plaintiff and class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

31. The U.S. Government Accountability Office noted in a report on data breaches (the "GAO Report") that identity thieves often use identifying data such as Social Security numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is particularly harmful because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim for years.

32. In addition, the GAO Report states that victims of identity theft may face "substantial costs and inconveniences repairing damage to their credit records."[5] Identity theft victims are frequently required to spend many hours, as well as money, repairing the impact to their credit.

---

[4] *See* https://www.gao.gov/new.items/d07737.pdf.

[5] *Id.*

33. There may be a substantial time lag – measured in years – between when sensitive information is stolen and when it is used. According to the GAO Report: "[O]nce stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[6] Thus, Plaintiff and class members must vigilantly monitor their financial and medical accounts for many years to come.

34. With access to the type of information that was accessed in the Data Breach, criminals can open accounts in victims' names; receive medical services in the victims' name; obtain a driver's license or official identification card in the victim's name but with the thief's photo; use the victim's name and Social Security number to obtain government benefits; file a fraudulent tax return using the victim's information; and give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[7]

35. The Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell it on the cyber "black-market" or "dark web" indefinitely. Cyber criminals routinely post stolen Social Security numbers, financial information, medical information, and other sensitive personal information on anonymous websites, making the information widely to a criminal underworld. There is an active and robust market for this information.

36. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants knew or should have known this, and strengthened their data systems

---

[6] *Id.*

[7] *See* Federal Trade Commission, Warning Signs of Identity Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

V. CLASS ACTION ALLEGATIONS

37. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class and a Massachusetts Sub-Class (collectively, the "Classes"), defined as follows:

> Nationwide Class: All persons in the United States who utilized Quest's services and whose Sensitive Information was maintained on AMCA's system that was compromised in the data breach announced by Quest on June 3, 2019.
>
> Massachusetts Sub-Class: All persons in the State of Massachusetts who utilized Quest's services and whose Sensitive Information was maintained on AMCA's system that was compromised in the data breach announced by Quest on June 3, 2019.

38. Excluded from the above Classes are Defendants' executive officers, and the judge to whom this case is assigned.

39. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. The Nationwide Class consists of 11.9 million individuals. The Massachusetts Sub-Class consists of tens of thousands or more individuals, on information and belief.

40. Commonality. There are many questions of law and/or fact common to Plaintiff and the class. Common questions include, but are not limited to:

a. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

b. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendants owed a duty to class members to safeguard their Sensitive Information;

d. Whether Defendants breached their duty to class members to safeguard their Sensitive Information;

e. Whether computer hackers obtained class members' Sensitive Information in the Data Breach;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Plaintiff and class members suffered legally cognizable damages as a result of Defendant's misconduct; and

h. Whether Plaintiff and class members are entitled to injunctive relief.

41. Typicality. Plaintiff's claims are typical of the claims of class members in that Plaintiff, like all class members, had his personal information compromised in the Data Breach.

42. Adequacy of Representation. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable counsel with significant experience in complex class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiff's counsel has the financial and personnel resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to, or that conflict with, those of the Classes.

43. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and class members. The common issues arising from Defendants' conduct affecting class members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

44. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

45. Defendants have acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis under Fed. R. Civ. P. 23(b)(2).

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of the Nationwide Class and Massachusetts Sub-Class)

46. Plaintiff re-alleges and incorporates by reference all preceding allegations.

47. Quest required Plaintiff and class members to submit non-public personal information in order to obtain medical services, which it forwarded to Optum360 and/or AMCA for billing purposes.

48. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard class members' Sensitive Information, to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could

detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

49. Defendants owed a duty of care to Plaintiff and class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Sensitive Information.

50. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Quest and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

51. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

52. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

53. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

54. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect class members' Sensitive Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Sensitive Information;

b. Failing to adequately monitor the security of AMCA's networks and systems;

c. Failure by Quest to periodically ensure that its vendors, including Optum360 and AMCA, had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to class members' Sensitive Information;

e. Failing to detect in a timely manner that class members' Sensitive Information had been compromised; and

f. Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

55. It was foreseeable that Defendants' failure to use reasonable measures to protect class members' Sensitive Information would result in injury to class members. Further, the breach

of security was reasonably foreseeable given the known high frequency of data breaches in the medical industry.

56. It was therefore foreseeable that the failure to adequately safeguard class members' Sensitive Information would result in one or more types of injuries to class members.

57. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

58. Plaintiff and class members are also entitled to injunctive relief requiring Defendants to, *e.g.*,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT II

BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class and Massachusetts Sub-Class)

59. Plaintiff re-alleges and incorporates by reference all preceding allegations.

60. When Plaintiff and class members provided their Sensitive Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

61. Defendants solicited and invited class members to provide their Sensitive Information as part of Defendants' regular business practices. Plaintiff and class members accepted Defendants' offers and provided their Sensitive Information to Defendants.

62. In entering into such implied contracts, Plaintiff and class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

63. Class members were aware of, or reasonably anticipated that, Quest would forward certain Sensitive Information to vendors, as disclosed in Quest's Notice of Privacy Practices.

64. Class members who paid money to Quest reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

65. Plaintiff and class members would not have entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information reasonably secure. Plaintiff and class members would not have entrusted their Sensitive Information to Quest in the absence of Quest's implied promise to monitor its vendors to ensure that they adopted reasonable data security measures.

66. Plaintiff and class members fully and adequately performed their obligations under the implied contracts with Defendants.

67. Defendants breached their implied contracts class members by failing to safeguard and protect their Sensitive Information. Quest breached its implied contract with class members by failing to properly monitor the data security practices of its vendors, Defendants Optum360 and AMCA.

68. As a direct and proximate result of Defendants' breaches of the implied contracts, class members sustained damages as alleged herein.

69. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

70. Plaintiff and class members are also entitled to injunctive relief requiring Defendants to, *e.g.*,: (i) strengthen their data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT III

MASSACHUSETTS CONSUMER PROTECTION ACT,
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq*.
(On Behalf of the Massachusetts Sub-Class)

71. Plaintiff re-alleges and incorporates by reference all preceding allegations.

72. Plaintiff, members of the Massachusetts Sub-Class, and Defendants are each "persons" under Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

73. Defendants operate in "trade or commerce" under Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

74. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting residents of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

75. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including by:

a. Failing to implement and maintain reasonable data security measures to protect Massachusetts Sub-Class members' Sensitive Information;

b. Failing to identify foreseeable security risks, remediate the foreseeable risks, and improve data security measures in response to the countless well-publicized prior data breaches within the medical industry;

c. Failing to comply with statutory, regulatory, and common law duties pertaining to the security of Massachusetts Sub-Class members' Sensitive Information, including duties imposed by HIPAA; the FTC Act at 15 U.S.C.

§ 45; and the Massachusetts Data Security statute and its implementing regulations at Mass. Gen. Laws Ann. Ch. 93H, § 2 and 201 Mass. Code Regs. 17.01-05;

d. Misrepresenting that they would reasonably protect the confidentiality of class members' personal information;

e. Misrepresenting that they would comply with legal duties pertaining to the security of class members' personal information; and

f. Omitting, suppressing, and concealing the material fact that they did not adopt reasonable measures to secure class members' personal information.

76. Defendants' acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendants held the true facts about their inadequate data security measures, which Plaintiff and the Massachusetts Sub-Class members could not independently discover.

77. Plaintiff and Massachusetts Sub-Class members could not have reasonably avoided injury because Defendants' acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from patients about the inadequacy of their data security systems, Defendants created an asymmetry of information between them and patients that precluded patients from taking action to avoid or mitigate injury.

78. Defendants' inadequate data security practices had no countervailing benefit to patients or to competition.

79. Defendants mislead Plaintiff and Massachusetts Sub-Class members to induce them to rely on Defendants' misrepresentations and omissions in conducting business with Defendants.

80. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of class members' Sensitive Information.

81. Defendants acted intentionally, knowingly, and/or maliciously in violating the Massachusetts Consumer Protection Act, and recklessly disregarded Plaintiff's and Massachusetts Sub-Class members' rights.

82. Defendants were on notice of the high risk of data breaches within the medical industry generally and within their own businesses specifically.

83. As a direct and proximate result of Defendants' unfair and deceptive acts, Plaintiff and Massachusetts Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and/or monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Sensitive Information; and benefit of the bargain damages for class members who paid money for Quest's services.

84. Plaintiff and Massachusetts Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages, consequential damages, exemplary damages, injunctive or other equitable relief, and attorneys' fees and costs.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendants including the following:

A. Determining that this matter may proceed as a class action and certifying the classes asserted herein;

B. Appointing Plaintiff as representative of each of the classes and Plaintiff's counsel as class counsel;

C. An award to Plaintiffs and the Classes of compensatory and consequential damages;

D. Injunctive relief requiring Defendants to, *e.g.*,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members;

E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Such other or further relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: June 6, 2019

Respectfully submitted,

/s/ Peter S. Pearlman

Peter S. Pearlman
COHN LIFLAND PEARLMAN HERRMANN & KNOPF LLP
Park 80 West – Plaza One
250 Pehle Avenue, Suite 401
Saddle Brook, NJ 07663
Tel.: (201) 845-9600
Fax: (201) 845-9423
psp@njlawfirm.com

Sherrie Savett
Shanon Carson
Jon Lambiras
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel.: (215) 875-3000
Fax: (215) 875-4604
ssavett@bm.net
scarson@bm.net
jlambiras@bm.net

Counsel for Plaintiff and the Classes